A process flow diagram elucidating the entire onboarding process of AUA/KUA is as shown below:-

Enquiry made by applicant to UIDAI onboarding team

- **Step 1**: Submission of application form for appointment as AUA/KUA by applicant
- **Step 2**: Generation of unique application ID

Failure to fulfill procedure within said timeline

- **Step 3**: Issue of In-Principle approval letter to the applicant along with list of appendices
  - ✓ AUA Agreement **V 6.0**
  - ✓ Invoice for payment of License Fee
  - ✓ Invoice for payment of Pre-Onboarding Audit Fee
  - ✓ Pre-onboarding Audit Compliance Checklist
  - ✓ Statement and undertaking regarding authentication transaction volume
  - ✓ IS Audit Compliance Checklist

- **Step 4**: Undertaking Pre-onboarding Audit as per compliance check-list by CERT-IN empanelled auditor assigned by UIDAI
- **Step 5**: Submission of report & artefacts and obtaining approval from UIDAI (Status to be highlighted as "**Audit Report Under Review**" during interim and "**Approved**" once final approval is provided by UIDAI, access to be provided to entity and UIDAI assigned auditor)

Timeline to fulfill the procedures **within 90 days from date of issue of in-principle approval.** Applicant to be intimated regarding revoking of application in case of failure to fulfill within said timeline

- **Step 6**: Execution of AUA/KUA Agreement (Submission and verification Bank Guarantee in case of non-govt. entities)

- **Step 7**: Issue of pre-production access key and mapping of entity under Pre-Production environment.
- **Step 8:** Mandated no. of test transactions by each modality to be carried out by the entity using pre-production key and validation of the same by Tech Centre (authentication support) team
- **Step 9**: Intimation to Tech Centre team to validate once mandated no. of test transaction is completed by applicant

Timeline to fulfill the procedures **within 30 days.** Reminder mail to be sent to applicant for failing to comply either procedure

+

- **Step 10**: Undertaking IS Audit by CERT-IN empanelled auditor as per compliance check-list, followed by submission of report & artefacts. (Status to be highlighted as "**Audit Report Under Review**" during interim and "**Approved**" once final approval is provided by UIDAI, access to be provided to entity and auditor. Access to be blocked for UIDAI assigned auditor)

- **Step 12**: Migration of entity to Live Production

Application form
for
Appointment as Authentication User Agency (AUA) and e-KYC User Agency (KUA)

To:

  The Chief Executive Officer, Unique Identification Authority of India
  [Attention: Deputy Director (Authentication-II), UIDAI]
  UIDAI Head Office, Bangla Sahib Road

1. Details of the applicantMinistry, Department, secretariat, office or agency of the Central Government, a State Government or the Government/Administration of a Union territory, or other entity:	
(a) Name of the applicant[1]	
(b) Registration/ Incorporation No.[2] *(Please attach copy of the document, if applicable)*	
(c) License No.[3] *(Please attach copy of the document, if applicable)*	
(d) Registered office address	
(e) Correspondence address *{If other than address mentioned against (d)}*	
(f) GSTN registration number of the applicant,as per Form GST REG-06 *(Please attach copy of the document, if applicable)*	
(g) Tax Deduction and Collection Account Number(TAN) of the applicant *(Please attach copy of the document, if*	

1Name of the applicant Ministry, Department, secretariat, office or agency of the Central Government or the Government of State or Union territory, or other applicant entity

2 Copy of Certificate of incorporation/registration to be attached in case of "other than Govt. entities"

3 Copy of Certificate of Registration/License from the concerned Regulator issued from RBI, SEBI, IRDAI and PFRDA

	applicable)	
(h)	Type of Aadhaar Authentication facility; Corresponding category of requesting entity (*Tick as applicable*)	☐ Yes/No Authentication facility; AUA ☐ Yes/No Authentication facility and e-KYC Authentication facility; AUA and KUA
(i)	Board resolution/minutes (or other valid letter/instrument of authorisation)citing approval for submitting the application form, signing Authentication User Agency Agreement and doing other acts in relation to the same (*Please attach certified copy of the document*)	
(j)	The provision of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 under which authentication is required/permitted *{If such provision is section 7 or section 4(4)(b)(ii) or section 4(4)(b)(i) read with the Prevention of Money-laundering Act, 2002, please attach copy of the relevant notification published in the Official Gazette}*	☐ Section 7 ☐ Section 4(4)(b)(i), read with the Prevention of Money-laundering Act, 2002 ☐ Section 4(4)(b)(i), read with relevant Central Act other than the Prevention of Money-laundering Act, 2002 ☐ Section 4(4)(b)(ii) ☐ Section 4(7)
(k)	Category of the applicant Ministry/Department/ secretariat/office/agency/entity	☐ AMinistry, Department, secretariat, office, or agency of the Central Government, which has required, in terms of the provisions of section 7 of the Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of India ☐ A Ministry, Department, secretariat, office or agency of the Government of _____[4], which requires, in terms of the provisions of section 7 of Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of State ☐ An entity permitted under sub-clause (i) of clause (b)

---

4 Name of the concerned State, or the concerned Union territory with Legislature

of sub-section (4) of section 4 of the Act to offer authentication services under[5] of _____[6].

☐ An entity permitted under sub-clause (i) of clause (b) of sub-section (4) of section 4 of the Act to offer authentication services under section 11A of the Prevention of Money-laundering Act, 2002, by virtue of being a reporting entity under the said Act as a _____[7], in terms of _____[8] of sub-section (1) of section 2 of the said Act.

☐ An entity that has been allowed/authorised under sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Act, vide Ministry of Electronics and Information Technology's letter no. _____[9], dated _____[10].

☐ An entity that is required, in terms of the provisions of sub-section (7) of section 4 of the Act, to perform mandatory authentication by _____ of _____[11].

2. Contact details:

(a) Management Point of Contact (MPOC)		Person authorised on the basis of Board resolution/minutes (or other valid letter/instrument of authorisation)	Other key personnel (if any)
Name			
Full designation			

---

5 Reference of the relevant provision (section, sub-section, clause etc.) of the relevant Act of Parliament, other than the Prevention of Money-laundering Act, 2002 ("PML Act")

6 Name of the relevant Act of Parliament, other than the PML Act

7 banking company, or financial institution, or intermediary, or a person carrying on activities for playing games of chance for cash or kind, or Inspector-General of Registration appointed under section 3 of the Registration Act, 1908, or Central-Government-notified real estate agent, or Central-Government-notified dealer in precious metals, precious stones and other high value goods, or Central-Government-notified person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, or Central-Government-notified person carrying on such other activities (whichever is applicable)

8 clause (wa), or sub-clause (i) of clause (sa), or sub-clause (ii) of clause (sa), or sub-clause (iii) of clause (sa), or sub-clause (iv) of clause (sa), or sub-clause (v) of clause (sa), or sub-clause (vi) of clause (sa) (whichever is applicable)

9 Number of the letter so allowing/authorising

10 Date of the letter so allowing/authorising

11 the provision (section, sub-section, clause etc.) of the Act made by Parliament, other than the Aadhaar Act

Official email address			
Mobile number			
Alternate office/telephone number			
(b) Technical Point of Contact (TPOC)	CXO/ Head of the functional vertical, who reports to the chief executive or governing body of the applicant Ministry/ Department/secretariat/office/agency/entity		Other key personnel (if any)
Name			
Full designation			
Official email address			
Mobile number			
Alternate office telephone number			
(c) AUA/KUA infrastructure details	DC (Data Centre)		DR (Data Recovery Centre)
MPOC/TPOC Name			
Email address			
Telephone/Mobile No.			
Address			
District			
State			
PIN Code			
(d) Contact details for grievance redressal:			
(i) Website URL			
(ii) Email address			

(iii) Helpdesk number		

3. Details of Authentication Service Agency (ASA)

(a)	Name(s) of ASA (*In case of multiple ASAs, please provide their names*)	1. _____ 2. _____ 3. _____
(b)	Declaration by the ASA(s) agreeing to provide its/their secure network connectivity and related services for the performance of authentication (*Please attach letter of ASA in original)*	

4. Authentication requirements

(a)	Territorial extent for use of Authentication facility	☐ Whole of India
		☐ Name of State(s) and Union Territory(s):
(b)	Whether Authentication will be used to establish identity for carrying out financial transaction	☐ Yes ☐ No
(c)	Device form factor (*select one or more option*)	☐ Discrete Biometric Device ☐ Integrated Biometric Device ☐ Laptop/Desktop ☐ Mobile phone
(d)	Whether Authentication will be operator-assisted or by the user himself/herself (*selectone or more option*)	☐ Operator-assisted use ☐ Self-use

(e)	Mode of Authentication *(selectone or more option)*	☐ Demographic ☐ Fingerprint ☐ Face	☐ DTP ☐ Iris
(f)	Connectivity supported between AUA/KUA and ASA *(selectone or more option)*	☐ VPN ☐ Other; Please specify: _____	☐ Leased line
(g)	Confirmation that the applicant has perused and understood UIDAI's Information Security Policy – External Ecosystem – Authentication User Agency/ KYC User Agency v6.0 *(Copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached)*	☐ Yes ☐ No	
(h)	Confirmation that the applicant has perused and understood UIDAI's Model Privacy Policy for Protecting Personal data of Aadhaar Number Holders by Requesting Entities *(Copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached)*	☐ Yes ☐ No	

Gole Market, New Delhi – 110 001

Declarationsand Undertakings:

It is hereby declared that the information furnished in this application form is true and correct to the best of its knowledge and that no material particulars or information have been concealed or withheld,and that the _____ (name of applicant Ministry/Department/secretariat/office/agency/entity) hereby undertakes—

(a) to abide by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") and the regulations made thereunder;

(b) to facilitate, on receipt of in-principle approval from UIDAI, audit as per UIDAI "Compliance Checklist for Onboarding the Requesting Entity" and submit all compliance related documents attached as annexures before signing the AUA/KUA Agreement;

(c) to fulfil all requirements with respect to use of the Aadhaar Authentication facility as per the Aadhaar (Authentication and Offline Verification) Regulations, 2021;

(d) to set up and maintain within the territory of India,at all times, requisite infrastructure (including, but not limited to, servers, databases etc.) for the use of Aadhaar Authentication facilities, capable of handling a minimum of one lakh Authentication transactions per month;

(e) to carry out appropriate due diligence before engaging any sub-contractor, business correspondent or field operator for performing any functions in relation to the use of Aadhaar Authentication facilities, including onboarding of user/beneficiary/customer, Authentication application development, etc.;

(f) to store Aadhaar numbers, if authorised so to do, only in the Aadhaar Data Vault, in accordance with such policies, procedures, standards and technical specifications as UIDAI may specify from time to time;

(g) to ensure the carrying out of audit of its own operations and systems and those of its Sub-AUAs and Sub-KUAs, if any, as required under the Aadhaar Act,the regulations made thereunder and the AUA Agreement;

(h) to not share or disclose e-KYC data that may be received on use of e-KYC Authentication facility, except in accordance with the provisions of the Aadhaar Act and the regulations made thereunder; and

(i) to inform UIDAI forthwith of any change in the name, address and other particulars of the applicant and contact persons as furnished in this application form.

(Signature with stamp/seal of authorised signatory)

Name: _____

Full designation: _____

Date: _____

Place: _____

Compliance checklist for verification of information furnished by applicant for appointment as AUA/KUA

Version 1.0 [issued in March 2024]

Important note: Wherever a control description requires AUA/KUA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablements are in place to secure compliance with the same on an ongoing basis.

Control no.	Short title	Control description	Control mapping	Compliance status (Compliant / Non-compliant / Not applicable)	Auditor's observation	Comments of AUA/KUA management
A.	**Information security governance**					
1.	Security organisation and CISO function	AUA/KUA should ensure that it has a designated Chief Information Security Officer (CISO) function that oversees information security governance and compliances. The CISO should have independent reporting to its Board or other governing body or chief executive.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(1)			
2.	Appointment of management and technical single point of contact	AUA/KUA should appoint a Management Single Point of Contact (MPOC) and Technical Single Point of Contact (TPOC) that should oversee the management of the authentication application and Aadhaar related	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.3			

			activities.				
			MPOC/TPOC should ensure consistent communication with UIDAI on Aadhaar related requirements and compliances.				
			Any change in MPOC/TPOC should be communicated to UIDAI in a timely manner.				
3.		Information security policy and procedure	AUA/KUA should have an information security policy and information security procedures in accordance with industry leading standards, such as ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework and ISO27701 (PIMS). The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.9			

4.	Aadhaar authentication application design	AUA/KUA should ensure that the authentication application design architecture is documented and validated by UIDAI Technology Centre and covers Aadhaar security requirements.	UIDAI Information Security Policy —UIDAI External Ecosystem — Section 2.3(5)			
5.	Aadhaar authentication application design	AUA/KUA should ensure that the Aadhaar data flow is properly documented for its AUA/KUA applications and those of its Sub-AUAs and Sub-KUAs.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(6)			
6.	Risk assessment	AUA/KUA should implement process and procedure to perform periodic (atleast annual) information security risk assessment of its ICT infrastructure supporting the authentication application. Further, entity should also perform risk assessment of its third party suppliers / vendors having access to the Aadhaar application and the data of Aadhaar number holders.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(13)			

		Security risks should be documented and reviewed periodically by Security Officers / CISO / those incharge of the security governance of the AUA/KUA and its Sub-AUAs and Sub-KUAs.				
7.	Third party information security policy	AUA/KUA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (*e.g.,* third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud service providers etc.) are obligated to adhere to.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(14)			
B.	**Compliance requirement**					
8.	IPR provisionsco ntained in UIDAI's Aadhaar User AgencyAgre ement (latest version)	The AUA/KUA should be in compliance with the intellectual property provisions contained in UIDAI's Aadhaar User Agency	Authentication User Agency Agreement version 6.0 — Section 3			

		Agreement (latest version).				
9.	Annual information security audit by CERT-In-empanelled auditor	AUA/KUA should ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with UIDAI's standards and specifications. The audit report should be shared with UIDAI. If any non-compliance is found as a result of the audit, AUA/KUAshould — (a) determine the causes of the non-compliance; (b) evaluate the need for actions to avoid recurrence of the same; (c) determine and enforce the implementation of corrective and preventive actions; and	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (h) of sub-regulation (1) of regulation 14 • The Aadhaar (Data Security) Regulations, 2016 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			

		(d) review the corrective actions taken. The annual audit should cover all security controls applicable under the Aadhaar (Data Security) Regulations, 2016.				
10.	Onboarding of ASA	AUA/KUA should ensure that UIDAI is informed of the ASAs with whom it has entered into agreementto provide necessary infrastructure for ensuring secure network connectivity and related services to it to enable performance of authentication using the Authentication facilities provided by UIDAI.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III —Sub-clause (g) of sub-regulation (1) of regulation 14			
C.	**Data privacy**					
11.	Data protection policy	AUA/KUA should establish a data protection policy addressing, *inter alia,*data protection related aspects under— (a) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.14(2) • The IT Act • Till the coming into force of the DPDP Act, the SPDI Rules			

		UIDAI from time to time; (b) the Information Technology Act, 2000 ("IT Act"); and (c) till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of AUA/KUA and the URL for the same should be	and, on and from the date of coming into force of clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, the said Act and the rules made thereunder[12]			

[12]*See* clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, read with clause (ob) of sub-section (2) of section 87 and section 43A of the IT Act

		mentioned.				
12.	Consent of Aadhaar number holder	The AUA/KUA should obtain consent of the Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, before collecting their identity information for the purposes of authentication. The consent should be obtained preferably in electronic form.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II —Regulation 6			
13.	Information to Aadhaar number holder on the nature of information that will be shared upon performance of authentication	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the parent or legal guardian of such child,regarding the nature of information that will be shared by UIDAI upon performance of authentication.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II —Clause (a) of sub-regulation (1) of regulation 5			
14.	Information to Aadhaar number holder on use of information	At the time of authentication, before obtaining consent, AUA/KUA should inform the	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter			

	received during authenticatio n	Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, of the uses to which the information received during authentication may be put to by it.	II —Clause (b) of sub-regulation (1) of regulation 5			
15.	Alternative mechanisms for submission of identity information	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the parent or legal guardian of such child, of the alternatives to submission of identity information.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II —Clause (c) of sub-regulation (1) of regulation 5			
16.	Consent communicat ion in local language	The AUA/KUA should ensure that the consent information is communicated in local language. The AUA/KUA should also ensure that,on and from the date of coming into force of sub-section (3) of section 5 of the DPDP Act, the Aadhaar number holder has the option to access the contents of the	• The Aadhaar (Authenticatio n and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 5 • On and from the date of coming into force of sub-section (3) of section 5 and sub-section (3) of section 6 of the DPDP Act,			

		notice referred to in sub-sections (1) and (2) of the said sectionand the request for consent referred to in sub-section (3) of section 6in English or any language specified in the Eighth Schedule to the Constitution.	the said Act — Sub-section (3) of section 5 and sub-section (3) of section 6			
17.	Communication of consent related information to persons with visual/hearing disability	The AUA/KUA should make provisions for communication of consent related information to persons with visual/hearing disability in an appropriate manner.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.14			
18.	Explicit consent; no umbrella consent	AUA/KUA should ensure that the consent taken from the Aadhaar number holder should in accordance with the provisions of the Aadhaar Act, 2016 and the regulations made thereunder;no umbrella consent should be taken for sharing e-KYC or Aadhaar number of the Aadhaar number holders with other entities. The AUA/KUA should also ensure that,on and from the date of coming	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.9 • On and from the date of coming into force of sub-section (1) of section 5 and sub-section (1) of section 6 of the DPDP Act, the said Act — Sub-section (1) of section 5 and sub-section (1) of section 6			

		into force of sub-section (1)of section 5 and sub-section (1) of section 6 of the DPDP Act, the consent taken from the Aadhaar number holder is in accordance with the applicable provisions of sections 5 and 6 of the said Act.				
D.	**Asset management**					
19.	Biometric device management	AUA/KUA should capture the biometric information of the Aadhaar number holder using certified and registered biometric devices as per standards specified by UIDAI from time to time.	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause(a) of sub-regulation (1) of regulation 7, sub-regulation (1) of regulation 8 and clause (d) of sub-regulation (1) of regulation 14 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.4			

20.	End-point security	AUA/KUA should ensure that biometric deploying devices are connected with end-point systems that have the latest operating system (OS) specifications (as of March 2024, at least Windows 10 and above and Android OS 10 and above), and that systems based on an OS that is end-of-life or end-of-support are not deployed or used.	Advisory regarding strengthening of Biometric authentication security [AdvisoryF. no. 13043/2/2021-AUTH-1-HQ, dated 31.5.2022]			
21.	Security hardening of assets	AUA/KUA should ensure all the end-point devicesand assets are used only after hardening to reduce/eliminate the attack vector and condense the system attack surface.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
22.	Maintenance of software inventory	AUA/KUA should ensure that it uses only licensed software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			

23.	Asset disposal procedure	AUA/KUA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposedof securely.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.4			
E.	**Human resource security**					
24.	Background verification and signing of confidentiality agreement	AUA/KUA should conduct a background check and sign a confidentiality agreement/ non-disclosure agreement (NDA) with all personnel/agency handling Aadhaar related information. Access to authentication infrastructure should not be granted before signing NDA and completion of background verification(BGV) for personnel.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			
25.	Background verification and signing of confidentiality agreement with third-party	AUA/KUAshould take an undertaking from business correspondents (BCs) and similar entities, Sub-AUAs/Sub-KUAs	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

	contractors	and other third party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data.				
26.	Training and awareness	AUA/KUA should ensure that MPOC, TPOC and their supporting teams that manage and maintain the authentication application and its underlying infrastructure, are aware of Aadhaar security requirements.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(7)			
27.	Operator qualification	AUA/KUA should ensure that the operator employed for performing authentication functions and maintaining necessary systems, infrastructure and process, possess requisite qualification for undertaking such work.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III —Clause (f) of sub-regulation (1) of regulation 14			
28.	Periodic information security and privacy trainings related to Aadhaar authenticatio n operations	AUA/KUA should impart information security and data privacy trainings to all its personnel as well as those of any BCs, Sub-AUAs/Sub-KUAs and similar entities, in relation to the use of	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

		Aadhaar Authentication facilities, during induction of such personnel/entity, on half-yearly basis and as and when changes are made in the authentication ecosystem. AUA/KUA should further ensure that specific and specialised training are imparted for various functional roles involved in the authentication ecosystem and that the same cover all relevant security and data privacy guidelines, as per the UIDAI Information Security Policy for Authentication, Aadhaar Act, 2016 and the regulations made thereunder and circulars, notices etc. issued by UIDAI from time to time. AUA/KUA should also maintain a record of such trainings imparted.				
F.	**Incident management**					

29.	Incident management procedure and RCA procedure	AUA/KUA should ensure that incident management framework, including forensic investigation, is implemented in accordance with the requirements under UIDAI's Information Security Policy and circulars. AUA/KUA should perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub-contractors, if any.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.12 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			
30.	Incident reporting requirement for Sub-AUAs/Sub-KUAs and BCs	AUA/KUAshould ensure that the Sub-AUAs/Sub-KUAs, BCs and other sub-contractors are aware of Aadhaar authentication related incident reporting.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.12			
G.	**Access control**					
31.	Multi-factor authenticatio n of operator	AUA/KUA should ensure in the case of assisted devices and applications where operators need to mandatorily perform application functions, that the operator is authenticated using a multi-factor	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5			

		authentication scheme, such as user id, password, Aadhaar authentication, answer to personal security questions, soft token, hard token, one-time password, voice recognition, biometric data match and PIN.					
32.	Access provisioning mechanism	AUA/KUA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar processing related information.	• UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.5 • The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of regulation 5				
33.	Privilege user access management	AUA/KUA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (6)				

34.	Privilege accounts	AUA/KUA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator and root accounts, are accessible only to a limited set of users, and thataccess to privileged account is not allowed to normal users.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
35.	Periodic access review	AUA/KUA should ensure that access is provided based on least privilege and that access is reviewed periodically (at leasthalf-yearly).	• UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.5 (2) • The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of regulation 5			
36.	Segregation of duties	AUA/KUA should ensure that personnel involved in operational, development or testing functions should not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or processes that may	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9(4) and(5)			

		compromise data security. Where segregation of duties is not possible or practicable, the process should include compensating controls, such as monitoring of activities, maintenance and review of audit trails and management supervision.				
37.	Initial password allocation	AUA/KUA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first login.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.6 (1)			
38.	Password management guidelines	AUA/KUA should ensure that passwords set are complex, with a minimum length of eight characters and— (a) are not based on anything somebody else may easily guess or obtain using person related information, *e.g.,*	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.6 (5)			

		name, telephone number and date of birth; (b) is free of consecutive identical characters or all-numeric or all-alphabetica l groups; (c) contain at least one numeric, one uppercase letter, one lowercase letter and one special character; (d) are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords); (e) do not allow the use of the last five passwords; (f) do not allow the				

		username and password to be the same for a particular user; and (g) do not use the same password for various UIDAI access needs of a particular user.				
39.	User account lockout	AUA/KUA should ensure that three successive log-in failures result in the user account being locked. End users / operators should not be able to login until their account is unlocked and the password is reset.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (9)			
40.	Restriction usage of generic IDs	AUA/KUA should ensure that common or generic or group user IDs are not used.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (5)			
H.	**Change management**					
41.	Change logs management	AUA/KUA should document all changes to Aadhaar authentication applications, infrastructure, processes and information processing	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.15 (1)			

		facilities, and maintain change log/register.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.15 (2)			
I.	**Data security**					
42.	Use of Aadhaar data vault (ADV) on cloud	AUA/KUA should ensure that if ADV is hosted on cloud, the ADV cloud service complies with UIDAI's Guidelines for ADV on Cloud. The ADV should be hosted only by Government Community Cloud (GCC) service providers, recognised as such by the Ministry of Electronics and Information Technology.	UIDAI Guidelines for ADV on Cloud			
43.	End-point security	AUA/KUA should ensure that USB access on the servers and endpoints is, in the default, restricted for all, and the same is allowed only on approval basis.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
44.	End-point security — antivirus / anti-malware	AUA/KUA should use licensed malware and antivirus solution (preferablyNext-Generation antivirus) to	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9(10)			

		protect against malware. The malware/antivirus installed should be configured to update in real time.				
45.	Use of security communicat ion protocols	AUA/KUA and ASA should ensure message security and integrity between their servers and those of third party entities, such as Sub-AUAs and Sub-KUAs. AUA/KUA should procure digital certificate from a Certifying Authority as defined in the IT Act.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(6)			
46.	End-point security	AUA/KUA should ensure that end-point devices used for developing, process and handling Aadhaar data and application timeout after a session is idle for more than 30 to 15 minutes, based on the criticality of the application.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(29) • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(30)			

47.	Secure software development	AUA/KUA should implement system and processes to ensure secure software development practices. Periodic training of developers should be conducted on secure software development practices. Records of such trainings should be maintained.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.9(5)			
48.	Patch management	AUA/KUA should ensure that the patch management process is implemented for applying patches to information systems. Patches should be updated at both the application and the server and network levels. AUA/KUA should ensure that either N or N-1 patches are maintained.	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9(8)			
J.	**Network security**					
49.	Network security	AUA/KUA should ensure that Internet access on systems are restricted to necessary or work-related websites and that access to web portals known for pirated software, gambling etc. are restricted.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			

K.	**Operations security**					
50.	Restrictions on designing/ compiling malicious code	AUA/KUA personnel should not intentionally write, generate, compile, copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any Aadhaar information.	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9			
51.	Implementation of Virtual ID	AUA/KUA must provide in their authentication application the option for an Aadhaar number holderto use a Virtual ID (VID) for authentication, in place of their Aadhaar number.	UIDAI circular no. K-11020/217/2018-UIDAI (Auth-I), dated 1.5.2018 (Implementation of VID, UID Token and Limited KYC)			
52.	Establishment of grievance handling mechanism	AUA/KUA should have an effective grievance handling mechanism and provide the same through multiple channels.	Authentication User Agency Agreement version 6.0 — Paragraph 14.3			
L.	**Application security**					
53.	Compliance to API specifications and application security	AUA/KUA should ensure that the client applications and software used for authentication should conform to the latest API standards and specifications laid down by UIDAI from time to time, and that itsSub-	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 8 and Chapter III — Clause			

		AUAs and Sub-KUAs use client applications or software development kit (SDK) developed or digitally signed by the AUA/KUA.	(a) of sub-regulation (3) of regulation 15 • UIDAI Aadhaar Authentication Application Security Standard, version 1.0, 2020 • UIDAI Aadhaar Authentication API Specification Version 2.5, Revision 1, January 2022			
54.	API whitelisting and API gateway implementation	AUA/KUA should ensure that it has API whitelist implemented to limit the data exchange using only authorised APIs and with whitelisted IP addresses. AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(4)			

| | | API and Distributed Denial of Service (DDoS) attacks.

AUA/KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the clientside. | | | | |
|---|---|---|---|---|---|---|
| 55. | Vulnerability assessment | AUA/KUA should plan organisation information security policy, inclusive of vulnerability assessment and penetration testing on its network, infrastructure and applications. | UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(6) | | | |
| 56. | Configuration reviews and system walkthrough | AUA/KUA should ensure that authentication applications are integrated with IDAM, PIM/PAM and SIEM. | UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(8) | | | |
| 57. | Application code review | AUA/KUA should ensure that the passwords, tokens, security keys and licenses are not hardcoded in the application code. | UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(5) | | | |
| **M.** | **Logging and monitoring** | | | | | |
| 58. | Clock synchronisation through use of Network | AUA/KUA should connect to the Network Time Protocol (NTP) server of the | • UIDAI Information Security Policy— UIDAI | | | |

		Time Protocol (NTP)	National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to the said NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC; however, it should be ensured that such time source does not deviate from NPL and NIC.	External Ecosystem — AUA KUA — Section 2.9 (22) • CERT-In Directive No. 20(3)/2022-CERT-In dated 28.4.2022			
N.	**Providing Aadhaar Authentication facilities to Sub-AUAs and Sub-KUAs**						
59.	Authenticati on application security	AUA/KUA should ensure that the authentication application to be used or being used for Aadhaar authentication by its Sub-AUAs and Sub-KUAs is developed and be digitally signed by AUA/KUA.	UIDAI Circular K11022/460/201 6-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(i)			
60.	Authenticati on application security	AUA/KUA should ensure that the authentication application used by its Sub-AUAs and Sub-KUAs does not store biometric data under any	UIDAI Circular K11022/460/201 6-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(ii)			

		circumstance, and that the biometrics / PID block is encrypted at the front-end device / client level.				

***

Compliance checklist for certifying compliance with controls that the AUA/KUA is required to have in place

Version 1.0 [issued in March 2024]

Important note: Wherever a control description requires AUA/KUA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablements are in place to secure compliance with the same on an ongoing basis.

Control no.	Short title	Control description	Control mapping	Compliance status (Compliant / Non-compliant / Not applicable)	Auditor's observation	Comments of AUA/KUA management
A.	**Information security governance**					
1.	Security organisation and CISO function	AUA/KUA should ensure that it has a designated Chief Information Security Officer (CISO) function that oversees information security governance and compliances. The CISO should have independent reporting to its Board or other governing body or chief executive.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(1)			
2.	Appointment of management and technical single point of contact	AUA/KUA should appoint a Management Single Point of Contact (MPOC) and Technical Single Point of Contact (TPOC) that should oversee the management of the authentication	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

		application and Aadhaar related activities. MPOC/TPOC should ensure consistent communication with UIDAI on Aadhaar related requirements and compliances. Any change in MPOC/TPOC should be communicated to UIDAI in a timely manner.				
3.	Information security policy and procedure	AUA/KUA should have an information security policy and information security procedures in accordance with industry leading standards, such as ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework and ISO27701 (PIMS). The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.9			

4.	Aadhaar authentication application design	AUA/KUA should ensure that the authentication application design architecture is documented and validated by UIDAI Technology Centre and covers Aadhaar security requirements.	UIDAI Information Security Policy —UIDAI External Ecosystem — Section 2.3(5)			
5.	Aadhaar authentication application design	AUA/KUA should ensure that the Aadhaar data flow is properly documented for its AUA/KUA applications and those of its Sub-AUAs and Sub-KUAs.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(6)			
6.	Risk assessment	AUA/KUA should implement process and procedure to perform periodic (at least annual) information security risk assessment of its ICT infrastructure supporting the authentication application. Further, entity should also perform risk assessment of its third party suppliers / vendors having access to the Aadhaar application and the data of Aadhaar number holders. Security risks	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(13)			

		should be documented and reviewed periodically by Security Officers / CISO / those in charge of the security governance of the AUA/KUA and its Sub-AUAs and Sub-KUAs.				
7.	Third party information security policy	AUA/KUA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (*e.g.,* third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud service providers etc.) are obligated to adhere to.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(14)			
B.	**Compliance requirement**					
8.	IPR provisions contained in UIDAI's Aadhaar User Agency Agreement (latest version)	The AUA/KUA should be in compliance with the intellectual property provisions contained in UIDAI's Aadhaar User Agency Agreement (latest version).	Authentication User Agency Agreement version 6.0 — Section 3			

9.	Annual information security audit by CERT-In-empanelled auditor	AUA/KUA should ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with UIDAI's standards and specifications. The audit report should be shared with UIDAI. If any non-compliance is found as a result of the audit, AUA/KUA should— (e) determine the causes of the non-compliance; (f) evaluate the need for actions to avoid recurrence of the same; (g) determine and enforce the implementation of corrective and preventive actions; and (h) review the corrective actions taken. The annual audit should cover all	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (h) of sub-regulation (1) of regulation 14 • The Aadhaar (Data Security) Regulations, 2016 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			

		security controls applicable under the Aadhaar (Data Security) Regulations, 2016.				
10.	Onboarding of ASA	AUA/KUA should ensure that UIDAI is informed of the ASAs with whom it has entered into agreement to provide necessary infrastructure for ensuring secure network connectivity and related services to it to enable performance of authentication using the Authentication facilities provided by UIDAI.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Sub-clause (g) of sub-regulation (1) of regulation 14			
11.	Annual compliance audit of Sub-AUAs and Sub-KUAs	AUA/KUA should ensure that the operations and systems of its Sub-AUAs and Sub-KUAs are audited on an annual basis by an information systems auditor certified by a recognised body, to ensure compliance with such standards and specifications as UIDAI may specify from time to time and that the audit report is shared with UIDAI.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.13			
C.	**Data privacy**					

12.	Data protection policy	AUA/KUA should establish a data protection policy addressing, *inter alia,* data protection related aspects under— (d) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by UIDAI from time to time; (e) the Information Technology Act, 2000 ("IT Act"); and (f) till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.14(2) • The IT Act • Till the coming into force of the DPDP Act, the SPDI Rules and, on and from the date of coming into force of clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, the said Act and the rules made thereunder[13]			

---

[13] *See* clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, read with clause (ob) of sub-section (2) of section 87 and section 43A of the IT Act

		the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of AUA/KUA and the URL for the same should be mentioned.				
13.	Consent of Aadhaar number holder	The AUA/KUA should obtain consent of the Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, before collecting their identity information for the purposes of authentication. The consent should be obtained preferably in electronic form.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Regulation 6			
14.	Information to Aadhaar number holder on the nature of information that will be shared upon performance of authentication	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the parent or legal guardian of such child, regarding the nature of information that will be shared by	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause (a) of sub-regulation (1) of regulation 5			

		UIDAI upon performance of authentication.				
15.	Information to Aadhaar number holder on use of information received during authentication	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, of the uses to which the information received during authentication may be put to by it.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause (b) of sub-regulation (1) of regulation 5			
16.	Alternative mechanisms for submission of identity information	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the parent or legal guardian of such child, of the alternatives to submission of identity information.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause (c) of sub-regulation (1) of regulation 5			
17.	Consent communication in local language	The AUA/KUA should ensure that the consent information is communicated in local language. The AUA/KUA should also ensure that, on and from the date of coming into force of sub-	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 5			

		section (3) of section 5 of the DPDP Act, the Aadhaar number holder has the option to access the contents of the notice referred to in sub-sections (1) and (2) of the said section and the request for consent referred to in sub-section (3) of section 6in English or any language specified in the Eighth Schedule to the Constitution.	On and from the date of coming into force of sub-section (3) of section 5 and sub-section (3) of section 6 of the DPDP Act, the said Act — Sub-section (3) of section 5 and sub-section (3) of section 6			
18.	Communication of consent related information to persons with visual/hearing disability	The AUA/KUA should make provisions for communication of consent related information to persons with visual/hearing disability in an appropriate manner.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.14			
19.	Consent log retention	AUA/KUA should maintain the logs for— (a) record of consent of the Aadhaar number holder for authenticati on; and (b) record of disclosure of information , as mentioned in Control	• The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 6 • The Aadhaar (Authenticati on and Offline Verification)			

		numbers 13, 14, 15, 16, 17 and 18 above, to the Aadhaar number holder at the time of authentication. For any given Aadhaar number holder, whose identity information was collected, the AUA/KUA should be able to demonstrate that consent was taken and disclosure of information was made.	Regulations, 2021 — Chapter III — Clause (d) of sub-regulation (1) of regulation 18 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.14			
20.	Explicit consent; no umbrella consent	AUA/KUA should ensure that the consent taken from the Aadhaar number holder should in accordance with the provisions of the Aadhaar Act, 2016 and the regulations made thereunder;no umbrella consent should be taken for sharing e-KYC or Aadhaar number of the Aadhaar number holders with other entities. The AUA/KUA should also ensure that, on and from	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.9 • On and from the date of coming into force of sub-section (1) of section 5 and sub-section (1) of section 6 of the DPDP Act, the said Act — Sub-section (1) of			

		the date of coming into force of sub-section (1) of section 5 and sub-section (1) of section 6 of the DPDP Act, the consent taken from the Aadhaar number holder is in accordance with the applicable provisions of sections 5 and 6 of the said Act.	section 5 and sub-section (1) of section 6			
D.	**Asset management**					
21.	Biometric device management	AUA/KUA should capture the biometric information of the Aadhaar number holder using certified and registered biometric devices as per standards specified by UIDAI from time to time.	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause (a) of sub-regulation (1) of regulation 7, sub-regulation (1) of regulation 8 and clause (d) of sub-regulation (1) of regulation 14 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.4			

22.	Biometric device management	Devices reportingtransactions at a very low frequency over time may be potential targets of frauds. Therefore, AUA/KUA should maintain oversight in respect of the same and identify and remove such devices from the system.	Advisory regarding strengthening of Biometric authentication security [Advisory F. no. 13043/2/2021-AUTH-1-HQ, dated 31.5.2022]			
23.	Biometric device management	AUA/KUAshould monitor the operations of its devices and equipment, on periodic basis, for compliance with the terms and conditions, standards, directions and specifications, issued and communicated by UIDAI from time to time.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (e) of sub-regulation (1) of regulation 14			
24.	Biometric device management	AUA/KUAshould carryout analysis of devices with high failure rates and replace them.	Advisory regarding strengthening of biometric authentication security [Advisory F. no. 13043/2/2021-AUTH-1-HQ, dated 31.5.2022]			
25.	End-point security	AUA/KUA should ensure that biometric deploying devices are connected with end-point systems that have the latest	Advisory regarding strengthening of Biometric authentication security [Advisory F. no.			

		operating system (OS) specifications (as of March 2024, at least Windows 10 and above and Android OS 10 and above), and that systems based on an OS that is end-of-life or end-of-support are not deployed or used.	13043/2/2021-AUTH-1-HQ, dated 31.5.2022]			
26.	Security hardening of assets	AUA/KUA should ensure all the end-point devices and assets are used only after hardening to reduce/eliminate the attack vector and condense the system attack surface.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
27.	Asset inventory maintenance	AUA/KUA should ensure that all assets (business applications, operating systems, databases, network etc.) used for the purpose of delivering services to Aadhaar number holders using Aadhaar Authentication facilitiesare identified, labelled and classified.\n\nAUA/KUA should record the details regarding assets used and maintain and update the asset inventory on a continuous basis. Ownership of	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.4			

		authentication assets should be clearly documented.				
28.	Maintenance of software inventory	AUA/KUA should ensure that it uses only licensed software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			
29.	Asset disposal procedure	AUA/KUA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposed of securely.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.4			
30.	Asset repair procedure and asset movement logs	AUA/KUA should, before consigning any asset for repair, sanitise the same to ensure that it does not contain any Aadhaar related data. A register to log the movement of all the assetsconsigned outside should be maintained.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.4			
31.	Asset repair procedure	AUA/KUA should, in case of in-house repair of assets,	UIDAI Information Security Policy -			

		document the details of the original equipment manufacturer (OEM) and maintain the logs of the assets being repaired.	UIDAI External Ecosystem — AUA KUA — Section 2.4			
E.	**Human resource security**					
32.	Background verification and signing of confidentiality agreement	AUA/KUA should conduct a background check and sign a confidentiality agreement / non-disclosure agreement (NDA) with all personnel/agency handling Aadhaar related information. Access to authentication infrastructure should not be granted before signing NDA and completion of background verification (BGV) for personnel.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			
33.	Background verification and signing of confidentiality agreement with third-party contractors	AUA/KUA should take an undertaking from business correspondents (BCs) and similar entities, Sub-AUAs/Sub-KUAs and other third party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

34.	Training and awareness	AUA/KUA should ensure that MPOC, TPOC and their supporting teams that manage and maintain the authentication application and its underlying infrastructure, are aware of Aadhaar security requirements.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(7)			
35.	Operator qualification	AUA/KUA should ensure that the operator employed for performing authentication functions and maintaining necessary systems, infrastructure and process, possess requisite qualification for undertaking such work.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (f) of sub-regulation (1) of regulation 14			
36.	Periodic information security and privacy trainings related to Aadhaar authentication operations	AUA/KUA should impart information security and data privacy trainings to all its personnel as well as those of any BCs, Sub-AUAs/Sub-KUAs and similar entities, in relation to the use of Aadhaar Authentication facilities, during induction of such personnel/entity, on half-yearly basis and as and when changes are made in the authentication	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

		ecosystem. AUA/KUA should further ensure that specific and specialised training are imparted for various functional roles involved in the authentication ecosystem and that the same cover all relevant security and data privacy guidelines, as per the UIDAI Information Security Policy for Authentication, Aadhaar Act, 2016 and the regulations made thereunder and circulars, notices etc. issued by UIDAI from time to time. AUA/KUA should also maintain a record of such trainings imparted.				
F.	**Incident management**					
37.	Incident management procedure and RCA procedure	AUA/KUA should ensure that incident management framework, including forensic investigation, is implemented in accordance with the requirements under UIDAI's Information Security Policy and circulars. AUA/KUA should	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.12 • UIDAI Information Security Policy —			

		perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub-contractors, if any.	UIDAI External Ecosystem — AUA KUA — Section 2.13			
38.	Reporting of incidents to UIDAI and CERT-In	AUA/KUA should— (a) inform UIDAImisuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within its network, and report any confidentiality security breach of Aadhaar related information to UIDAI within 24 hours; (b) report cyber incidents as mentioned in Annexure I to the directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022-CERT-In, within 6 hours of noticing	• The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter III — Clause (l) of sub-regulation (1) of regulation 14 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Item 4 of section 2.12 • Directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022-CERT-In — Clause (ii) • DPDP Act — Sub-section (6) of section 8 and the rules under clause (f) of sub-			

		such incidents or the same being brought to their notice; and (c) on and from the date of coming into force of sub-section (6) of section 8 of the DPDP Act, intimation of personal data breach to the Board and each affected Data Principal, within such time as may be prescribed by rules made under the said Act.	section (2) of section 40			
39.	Incident reporting requirement for Sub-AUAs/Sub-KUAs and BCs	AUA/KUA should ensure that the Sub-AUAs/Sub-KUAs, BCs and other sub-contractors are aware of Aadhaar authentication related incident reporting.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.12			
G.	**Access control**					
40.	Multi-factor authentication of operator	AUA/KUA should ensure in the case of assisted devices and applications where operators need to mandatorily perform application functions, that the operator is authenticated using a multi-factor	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5			

		authentication scheme, such as user id, password, Aadhaar authentication, answer to personal security questions, soft token, hard token, one-time password, voice recognition, biometric data match and PIN.				
41.	Operator logs	AUA/KUA should maintain details of devices and operators employed for the use of Aadhaar Authentication facilities in assisted mode,including proper logs of such operators, along with their name, deviceID, date and time, etc. These logs should be verified by AUA/KUA at regular intervals.	Advisory regarding strengthening of biometric authentication security [Advisory F. no. 13043/2/2021-AUTH-1-HQ, dated 31.5.2022]			
42.	Access provisioning mechanism	AUA/KUA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 • The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of			

		processing related information.	regulation 5			
43.	Privilege user access management	AUA/KUA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (6)			
44.	Privilege accounts	AUA/KUA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator and root accounts, are accessible only to a limited set of users, and thataccess to privileged account is not allowed to normal users.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
45.	Periodic access review	AUA/KUA should ensure that access is provided based on least privilege and that access is reviewed periodically (at least half-yearly).	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (2) • The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of regulation 5			

46.	Access revocation mechanism	Within 24 hours of exit of any personnel, AUA/KUA should revoke the rights and privileges to access or process Aadhaar related information. Upon such revocation, user IDs should be deleted forthwith if not in use.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.3(8) and section 2.5			
47.	Segregation of duties	AUA/KUA should ensure that personnel involved in operational, development or testing functions should not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or processes that may compromise data security. Where segregation of duties is not possible or practicable, the process should include compensating controls, such as monitoring of activities, maintenance and review of audit trails and management supervision.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(4)and(5)			

48.	Initial password allocation	AUA/KUA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first log in.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.6 (1)			
49.	Password management guidelines	AUA/KUA should ensure that passwords set are complex, with a minimum length of eight characters and— (h) are not based on anything somebody else may easily guess or obtain using person related information, *e.g.,* name, telephone number and date of birth; (i) is free of consecutive identical characters or all-numeric or all-alphabetical groups; (j) contain at least one numeric, one uppercase letter, one	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.6 (5)			

		lowercase letter and one special character; (k) are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords); (l) do not allow the use of the last five passwords; (m) do not allow the username and password to be the same for a particular user; and (a) do not use the same password for various UIDAI access needs of a particular user.				
50.	User account lockout	AUA/KUA should ensure that three successive log-in failures result in the user account	UIDAI Information Security Policy — UIDAI External			

		being locked. End users / operators should not be able to log in until their account is unlocked and the password is reset.	Ecosystem — AUA KUA — Section 2.5 (9)			
51.	Restriction usage of generic IDs	AUA/KUA should ensure that common or generic or group user IDs are not used.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5(5)			
H.	**Change management**					
52.	Change logs management	AUA/KUA should document all changes to Aadhaar authentication applications, infrastructure, processes and information processing facilities, and maintain change log/register.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.15(1) • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.15(2)			
I.	**Physical security**					
53.	Physical security of AUA data centre	AUA/KUA data centre hosting Aadhaar related information should be secured fully and should have access control.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
54.	Security of	AUA/KUA should	UIDAI			

	AUA servers	ensure that their servers are placed in an isolated, secure cabinet in the data centre.	Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
55.	Physical security of AUA/KUAdata centre	AUA/KUA data centre and servers should be under 24X7protection of security guards and CCTV surveillance.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
56.	Physical security of AUA/KUA data centre	AUA/KUA should ensure that access to the data centre is restricted only to authorised individuals and appropriate logs of entry of individuals should be maintained.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
57.	Physical security of AUA/KUA data centre	AUA/KUA should ensure that physical access to the data centre and other restricted areas hosting critical Aadhaar related equipment/information is pre-approved and recorded, along with the date, time and purpose of entry.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
58.	Physical security of AUA/KUA data centre	AUA/KUA should ensure that the movement of all incoming and outgoing assets related to Aadhaar in the AUA/KUA data centre is documented.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			

59.	Physical security of AUA/KUA data centre	AUA/KUA should ensure that visible and clearly readable signs/notices notifying areas designated as restricted areas and provisions restricting entry to the same are posted at all points leading to entry to such areas.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
60.	Physical security of AUA/KUA data centre	AUA/KUA should provide lockable cabinets or safes in the data centre and information processing facilities for housing servers containing critical Aadhaar related information. AUA/KUA should deploy label, monitor and test regularly the operation of fire exit doors and fire extinguishing systems.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
61.	Preventive maintenance activity at data centre	AUA/KUA should ensure that preventive maintenance activities, such as audit of fire extinguishers and CCTV,are carried out on a quarterly basis.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.8			
62.	Physical location of AUA/KUA servers	AUA/KUAshould ensure thatthe data centres hosting servers on which	• The Aadhaar (Authenticati on and Offline			

		Aadhaar related information is stored are within India.	Verification) Regulations, 2021 — Chapter III — sub-regulation (1) of regulation 22 • UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9			
J.	**Data security**					
63.	PID encryption and biometric data security	AUA/KUA shouldensure that biometric data are necessarily encrypted and secured at the time of capture of such information of the Aadhaar number holder,in accordance with such specifications as UIDAI may lay down from time to time.	• The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 7 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.7			
64.	PID encryption and biometric data security	AUA/KUA should ensure that after collection of requisite demographic	• The Aadhaar (Authenticati on and Offline			

		and/or biometric information and/or one-time password (OTP) from the Aadhaar number holder, the client application immediately packages and encrypts these input parameters into a PID block, before transmitting the same, and that the same is sent to the server of the AUA/KUA using secure protocols.	Verification) Regulations, 2021 — Chapter II — Sub-regulation (1) of regulation 9 • The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (5) of regulation 9 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.7			
65.	PID encryption and biometric data security	AUA/KUA should ensure that the PID block is encrypted with a dynamic session key using AES 256 symmetric algorithm (AES/GCM/No Padding) at the time of capture on the authentication device. The session key should be encrypted with 2048-bit UIDAI	• UIDAI Aadhaar Authentication Application Security Standard • UIDAI Aadhaar Authentication API Specification Version 2.5			

		public key using asymmetric algorithm (RSA/ECB/PKCS1 Padding). In doing so, AUA/KUA should comply with the latest API specification document issued by UIDAIfrom time to time.				
66.	PID encryption and biometric data security	AUA/KUA should ensure with respect to the operational details referred to against control number 65, that the session key is not stored anywhere except in the memory and that the same is not reused across transactions. Reuse of session key is allowed only when it is used as seed key while using synchronised session key scheme.	• UIDAI Aadhaar Authentication Application Security Standard • UIDAI Aadhaar Authentication API Specification Version 2.5			
67.	Aadhaar number security	AUA/KUA should ensure that the Aadhaar number/ Virtual ID (VID) /ANCS token provided by the Aadhaar number holder for authentication request is not retained by the device operator or within the device or at the AUA/KUA	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (ca) of sub-regulation (1) of regulation 14			

		server(s).				
68.	Restriction in storage of Aadhaar number, biometrics and/or eKYC of Aadhaar number holder	AUA/KUA should ensure that under no circumstances assisted devices and any application associated with Aadhaar authentication stores the Aadhaar number, biometrics and/or e-KYC of the Aadhaar number holder.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (a) of sub-regulation (1) of regulation 17			
69.	Fingerprint biometric data (FMR and FIR) capture in single PID block	For fingerprint-based biometric authentication devices, AUA/KUA should ensure capture of Finger Minutiae Record (FMR) and Finger Image Record (FIR) in single PID block.	UIDAI circular K 11022/198/2017 -UIDAI (Auth-I), dated 11.11.2021			
70.	Security of private keys	AUA/KUA should ensure that the private key used for digitally signing the authentication request and the licence keys are kept secure and the access to the same is controlled, and that the private key meetssuch parametersas UIDAImay specify from time to time in the Aadhaar Authentication API Specification	Aadhaar Authentication API Specifications Version 2.5			

		document issued by it.				
71.	Use of HSM	AUA/KUA should ensure that key(s) used for digitally signing authentication requests and decrypting e-KYC XML responses are stored only in the Hardware Security Module (HSM), which should be compliant with the latest FIPS 140-2 standard. AUA/KUA should comply with all the requirements of UIDAI circular no. K 11020/204/2017-UIDAI (Auth-I), dated 22.6.2017 (Implementation of HSM by Entity/ASA).	UIDAI circular K 11020/204/2017 -UIDAI (Auth-I), dated 22.6.2017 (Implementation of HSM by Entity/ASA)			
72.	Use of HSM	AUA/KUA should have a dedicated, on-premise, HSM setup for the management of security/encryption keys,and should not share the same with any other entity.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.7(7)			
73.	Use of ADV	An AUA/KUAand any other entity which is allowed to store Aadhaar number should collect and store	UIDAI circular K-11020/205/2017 -UIDAI (Auth-I), dated 25.7.2017			

		Aadhaar number and any connected data only in a separate, secure database/vault/system, termed as Aadhaar Data Vault (ADV). Such AUA/KUA should ensure that each Aadhaar number is referred to by an additional key, called as reference key, and that mapping of the reference key and Aadhaar number is maintained in ADV.	(Circular for Aadhaar Data Vault)			
74.	Use of Aadhaar data vault (ADV) on cloud	AUA/KUA should ensure that if ADV is hosted on cloud, the ADV cloud service complies with UIDAI's Guidelines for ADV on Cloud. The ADV should be hosted only by Government Community Cloud (GCC) service providers, recognised as such by the Ministry of Electronics and Information Technology.	UIDAI Guidelines for ADV on Cloud			
75.	Use of ADV on cloud	AUA/KUA having ADV on cloud should get annual SOC2 Type II examination performed for cloud hosting	UIDAI Guidelines for ADV on cloud			

		service. Management review should be performed for non-compliant / qualified controls reported in the SOC2 Type II reports.				
76.	Use of ADV	AUA/KUA should ensure that Aadhaar numbers along with connected data (such as eKYC XML containing Aadhaar numbers and demographic data),if any, is stored only in a single logical instance of ADV, along with corresponding reference key. AUA/KUA should ensure that appropriate High Availability and Disaster Recovery provisions are made for the vault, with the same level of security.	UIDAI circular no. K-11020/205/2017 -UIDAI (Auth-I), dated 25.7.2017 (Circular for Aadhaar Data Vault)			
77.	Use of ADV	AUA/KUA should ensure that only trusted communications are permitted in and out of the vault; this should ideally be done through APIs/microservices dedicated to obtain the mapping and controlling the	UIDAI circular no. K-11020/205/2017 -UIDAI (Auth-I), dated 25.7.2017 (Circular for Aadhaar Data Vault)			

		access to the APIs/microservices at the application level. AUA/KUA should ensure that any authorised users needing to access such mapping necessarily go through the application for viewing/accessing the data, after appropriate user authentication, authorisation and logging.				
78.	Use of ADV	AUA/KUA should ensure that strong access controls, authentication measures, monitoring and logging of access and raising of necessary alerts for unusual and/or unauthorised attempts to access ADV are implemented.	UIDAI circular K-11020/205/2017-UIDAI (Auth-I), dated 25.7.2017 (Circular for Aadhaar Data Vault)			
79.	End-point security	AUA/KUA should ensure that USB access on the servers and endpoints is, in the default, restricted for all, and the same is allowed only on approval basis.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
80.	End-point security — antivirus / anti-malware	AUA/KUA should use licensed malware and antivirus solution	UIDAI Information Security Policy — UIDAI			

		(preferably Next-Generation antivirus) to protect against malware. The malware/antivirus installed should be configured to update in real time.	External Ecosystem — AUA KUA — Section 2.9(10)			
81.	Aadhaar information security — Physical Aadhaar documents	AUA/KUAshould mask Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters, by masking the first eight digits of the Aadhaar number, before storing physical copies.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (mb) of sub-regulation (1) of regulation (14)			
82.	Use of security communication protocols	AUA/KUA and ASA should ensure message security and integrity between their servers and those of third party entities, such as Sub-AUAs and Sub-KUAs. AUA/KUA should procure digital certificate from a Certifying Authority as defined in the IT Act.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(6)			
83.	Restriction on display/ publishing of identity information	AUA/KUA, Sub-AUAs, Sub-KUAs, Business Correspondents and other sub-contractors performing Aadhaar	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.9			

		authentication should ensure that identity information is not displayed or disclosed to external agencies or unauthorised persons.				
84.	Restriction in display/ publishing of identity information	AUA/KUA should not publish any personal identifiable data including Aadhaar in public domain/websites etc.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.9			
85.	Restriction in display/ publishing of identity information	AUA/KUA should ensure that display of full Aadhaar number is controlled only for the Aadhaar number holder or for such special roles/users of AUA/KUA as havefunctional necessity for the same; by default, all other display should be masked such that only the last four digits of the Aadhaar number are displayed.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.7(10)			
86.	End-point security	AUA/KUA should ensure that end-point devices used for developing, process and handling Aadhaar data and application timeout after a session is idle for more than	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(29)			

			30 to 15 minutes, based on the criticality of the application.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(30)			
87.	Secure software development	AUA/KUA should implement system and processes to ensure secure software development practices. Periodic training of developers should be conducted on secure software development practices. Records of such trainings should be maintained.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.9(5)				
88.	Restriction in local storage of Aadhaar data / PII information	AUA/KUA should ensure that there is no local storage of Aadhaar number or VID or the PID block on the system, volatile memory or the database. Incase of a mobile application, AUA/KUA should ensure that there is no local storage of Aadhaar number or the PID block in the shared preference folder.	• UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.9(19) • UIDAI circular no/ K-11020/217/2 018-UIDAI (Auth-I), dated 1.5.2018 (Implementat ion of Virtual ID, UID				

			Token and Limited KYC)			
89.	Encryption of stored eKYC data	AUA/KUA should ensure that e-KYC data is stored in an encrypted manner in database tables.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.9(18)			
90.	Patch management	AUA/KUA should ensure that the patch management process is implemented for applying patches to information systems. Patches should be updated at both the application and the server and network levels. AUA/KUA should ensure that either N or N-1 patches are maintained.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(8)			
K.	**Network security**					
91.	Network connectivity with ASA	AUA/KUA should establish secure network connectivity between AUA/KUA and its Sub-AUAs, Sub-KUAs, sub-contractors and ASAs, and should connect with ASAs only through secure leased lines or similar secure private lines. If a public network is used, only a secure channel should be	• The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter III — Clause (c) of sub-regulation (1) of regulation 14 • UIDAI Information Security Policy — UIDAI			

		used.	External Ecosystem —Sections 2.9 and 2.11			
92.	Segregation of AUA serversnetwork	AUA/KUAshoulde nsure that its servers reside in a segregated network segment isolated from the rest of the network of the AUA/KUA organisation. The AUA/KUA serversshould be dedicated for online Aadhaar authentication purposes and should not be used for any other activities not related to Aadhaar.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.9			
93.	Firewall access of network	AUA/KUA should ensure that authentication application servers and infrastructure are hosted behind a firewall and that firewall rules block incoming access requests to the AUA/KUA server from all sources other than whitelisted IP addresses/zones.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.11 (4)			
94.	NIPS/IDS implementation	AUA/KUA should ensure that network intrusion and prevention systems (NIPS) and intrusion detection system (IDS) are implemented to safeguard the	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9 (11)			

		network from external attacks / DDoS attacks.				
95.	Network security	AUA/KUA should ensure that Internet access on systems are restricted to necessary or work-related websites and that access to web portals known for pirated software, gambling etc. are restricted.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
96.	Encryption of data on network	AUA/KUA should ensure that transmission of Aadhaar number across open, public networks is always encrypted,using the latest version of Transport Layer Security (TLS)configuration.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(7)			
L.	**Operations security**					
97.	Segregation of testing and production environments	AUA/KUA should ensure that the testing and production facilities/environments are physically and/or logically separated. AUA/KUA should ensure that authentication application testing utilises test data / non-production data and thatAadhaar number holder's identity data are	UIDAI Information Security Policy - UIDAI External Ecosystem — AUA KUA — Section 2.9			

		not used for testing the application.				
98.	Restrictions on designing/ compiling malicious code	AUA/KUA personnel should not intentionally write, generate, compile, copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any Aadhaar information.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9			
99.	License key / encryption keys security	AUA/KUA should ensure that license keys are kept secure and access controlled, and that separate license keys are generated for their Sub-AUAs and Sub-KUAs from UIDAI's portal and kept secure and access to the same kept controlled.	• The Aadhaar (Authentica tion and Offline Verification) Regulations , 2021 — Chapter III — Sub-regulation (2) of regulation 15 • The Aadhaar (Authentica tion and Offline Verification) Regulations , 2021 — Chapter III — Clause (f) of sub-			

			regulation (1) of regulation 17 • UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.9			
100.	Implementation of Virtual ID	AUA/KUA must provide in their authentication application the option for an Aadhaar number holder to use a Virtual ID (VID) for authentication, in place of their Aadhaar number.	UIDAI circular no. K-11020/217/2018-UIDAI (Auth-I), dated 1.5.2018 (Implementation of VID, UID Token and Limited KYC)			
101.	UID Token	AUA/KUA should make provision to store UID tokens in their database.	UIDAI circular K-11020/217/2018-UIDAI (Auth-I), dated 1.5.2018 (Implementation of Virtual ID, UID Token and Limited KYC)			
102.	Restriction on the use of Aadhaar as domain-specific identifier	AUA/KUA should ensure that Aadhaar numberand VIDare never used as domain-specific identifiers and that domain-specific identifiers are revoked and/or reissued. For example, instead of	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.9			

		using Aadhaar number as bank customer ID or license number or student ID etc., a local, domain-specific identifier mapped in the back-end database should be used.				
103.	Unique device code of each device	AUA/KUA should ensure that each authentication device has a unique device code and that a unique transaction number is automatically generated by the authentication device and incremented for each transaction processed.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.11 (1)			
104.	Back-up / alternative identity authentication mechanism	AUA/KUA should implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to Aadhaar number holders.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (i) of sub-regulation (1) of regulation 14			
105.	Notification to Aadhaar number holders	AUA/KUA should notify the Aadhaar number holder of the success or failure of each authentication request, through email and/or SMS. Such notification should shall	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — sub-regulations (1), (2) and (3) of regulation 10			

		include the name of the requesting entity, the date and time of authentication, the authentication response code (in case of online authentication), the last four digits of the Aadhaar number and the purpose of authentication, as the case may be. In case of authentication failure, the AUA/KUA should, in clear and precise language, inform the Aadhaar number holderof the reasons of authentication failure, such as "Aadhaar cancelled", "Aadhaar deactivated", "Aadhaar locked", "Aadhaar omitted", "Aadhaar suspended" and "Biometrics locked".				
106.	Establishment of grievance handling mechanism	AUA/KUA should have an effective grievance handling mechanism and provide the same through multiple channels.	Authentication User Agency Agreement version 6.0 — Paragraph 14.3			

107.	Grievance handling mechanism of Sub-AUAs and Sub-KUAs	AUA/KUAshould ensure that its Sub-AUAs and Sub-KUAs have a grievance handling mechanism to receive and address complaints from Aadhaar number holders regarding authentication facilities performed by them.	Authentication User Agency Agreement version 6.0 — Paragraph 14.3			
108.	Aadhaar authentication for banks	Whereapplicable, AUA/KUA should comply with notification no. 13012/79/2017/Legal-UIDAI (No. 6 of 2017), dated 19.12.2017, regarding the process for placing and overriding bank accounts on Aadhaar Payments Bridge (APB) — National Payments Corporation of India (NPCI) Mapper. In particular, the AUA/KUA should comply with the following: (a) Override request pertaining to an Aadhaar number holder should be accompanied by the name of his/her	UIDAI Circular — Notification No. 13012/79/2017/ Legal-UIDAI (No. 6 of 2017), dated 19.12.2017			

		current bank on the APB mapper and confirmation from the requesting bank that it has obtained the requisite consent of the Aadhaar holder for switching to the requesting bank on the mapper. (b) Send request for mapping of a new account or overriding an existing bank account to NPCI only after taking explicit, informed consent of the customer. (c) Inform each accountholder through SMS and email, within 24 hours, that a request has been sent to NPCI to put his/her bank account on				

		the mapper or, as the case may be, to change his bank account on the NPCI mapper (while providing the name of current bank on the mapper and the last four digits of the account number of the new bank, along with the bank name) and, in case he/she does not want to put his/her new bank account on the mapper, provide the customer an option to reverse such mapping. (d) If an accountholder does not have an email or mobile number and communication cannot be sent, his/her					

		physical signature on a paper consent form should be obtained prior to sending the request to the NPCI mapper. (e) The records of consents obtained in (b) and the communications made in items (a), (b) and(c) and scanned copy of the consent form in (d) should be retained for seven years by the bank, in accordance withthe Aadhaar (Authentication and Offline Verification) Regulations, 2021. (f) Make available the aforesaid records at the time of audit, in accordance with the				

		Aadhaar (Authentication and Offline Verification) Regulations, 2021.				
M.	**Application security**					
109.	Compliance to API specifications and application security	AUA/KUA should ensure that the client applications and software used for authentication should conform to the latest API standards and specifications laid down by UIDAI from time to time, and that itsSub-AUAs and Sub-KUAs use client applications or software development kit (SDK) developed or digitally signed by the AUA/KUA.	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 8 and Chapter III — Clause (a) of sub-regulation (3) of regulation 15 • UIDAI Aadhaar Authentication Application Security Standard, version 1.0, 2020 • UIDAI Aadhaar Authentication API Specification Version 2.5, Revision 1, January 2022			

| 110. | API whitelisting and API gateway implementation | AUA/KUA should ensure that it has API whitelist implemented to limit the data exchange using only authorised APIs and with whitelisted IP addresses.

AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management.

AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDoS) attacks.

AUA/KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. | UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(4) | | | |
| 111. | Source code review by CERT-In- | AUA/KUA should perform source code review of the | UIDAI Information Security Policy | | | |

		modules and applications used for authentication and e-KYC and undergo audit by a CERT-In-empanelled auditor.	— UIDAI External Ecosystem — Section 2.10(5)			
112.	SAST/DAST application audit	AUA/KUA should ensure that authentication application security assessment {including static application security testing (SAST) and dynamic application security testing (DAST)} is performed at least annually or at the time of major changes to the authentication application, and that all vulnerabilities are addressed for remediation and no vulnerable third party components are used by the authentication application.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(6)			
113.	Vulnerability assessment	AUA/KUA should plan organisation information security policy, inclusive of vulnerability assessment and penetration testing on its network, infrastructure and applications.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(6)			
114.	Configuration reviews and system	AUA/KUA should ensure that authentication	UIDAI Information Security Policy			

	walkthrough	applications are integrated with IDAM, PIM/PAM and SIEM.	— UIDAI External Ecosystem — Section 2.11(8)			
115.	Application code review	AUA/KUA should ensure that the passwords, tokens, security keys and licenses are not hardcoded in the application code.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(5)			
N.	**Logging and monitoring**					
116.	Authentication log maintenance	AUA/KUA should maintain logs of the authentication transactions processed by it, which should contain the following transaction details: (a) specified parameters of authenticati on request submitted; (b) specified parameters received as authenticati on response; (c) the record of disclosure of information to the Aadhaar number holder at the time of authenticati on; and (d) record of consent of	• The Aadhaar (Authenticati on and Offline Verification) Regulations, 2021 — Chapter III — Sub-regulation (1) of regulation 18 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9 (15) • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9 (16)			

		the Aadhaar number holder for authentication, but shall not, in any event, retain the PID information, Aadhaar number/ VID.				
117.	Authentication log retention	AUA/KUA should ensure that the logs of authentication transactions are stored online for audit purposes for two years and, thereafter, archived for another five years.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — sub-regulations (2) and (3) of regulation 18			
118.	Retention of transaction logs of Sub-AUA/Sub-KUA	AUA/KUA should maintain auditable logs of all such transactions where e-KYC data has been shared with any of its Sub-AUAsand Sub-KUAs, for such period as UIDAI may specify from time to time.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Sub-regulation (6) of regulation 16			
119.	Security incident recording	AUA/KUA should ensure that the event/security logs recording critical user-activities, exceptions and security events are enabled and stored to assist any future investigation and enable access control monitoring.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(12)			

120.	Security incident monitoring	AUA/KUA should ensure that regular monitoring of event/security logs takes place to detect unauthorised use of information systems and that results of the same are recorded. Further, access to audit trails and event logs should be provided to authorised personnel only.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(13)			
121.	Clock synchronisation through use of Network Time Protocol (NTP)	AUA/KUA should connect to the Network Time Protocol (NTP) server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to the said NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC; however, it should be ensured that such time source does not deviate from NPL and NIC.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9 (22) • CERT-In Directive No. 20(3)/2022-CERT-In dated 28.4.2022			

O.	**Fraud and forensics**					
122.	Fraud analytics module	AUA/KUAshould deploy, as part of its systems, a fraud analytics module that is capable of analysing authentication related transactions to identify fraud.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13 (9)			
P.	**Providing Aadhaar Authentication facilities to Sub-AUAs and Sub-KUAs**					
123.	Approval from UIDAI for appointment of Sub-AUA/Sub-KUA	AUA/KUA should obtain approval from UIDAI before appointing any entity as its Sub-AUA or Sub-KUA, and should also take permission in respect of anyentity already appointed as a Sub-AUA or Sub-KUA.	UIDAI Information Security Policy—UIDAI External Ecosystem — AUA KUA — Section 2.13			
124.	Authentication application security	AUA/KUA should ensure that the authentication application to be used or being used for Aadhaar authentication by its Sub-AUAs and Sub-KUAs is developed and be digitally signed by AUA/KUA.	UIDAI Circular K11022/460/2016-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(i)			
125.	Authentication application security	AUA/KUA should ensure that the authentication application used by its Sub-AUAs and Sub-KUAs does not store biometric data under any circumstance, and that the biometrics / PID block is	UIDAI Circular K11022/460/2016-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(ii)			

		encrypted at the front-end device / client level.				
126.	Authentication application security	AUA/KUA should ensure that the client application(s) of its Sub-AUAs and Sub-KUAs does/do not, under any circumstance, replay the authentication request using stored biometric data.	UIDAI Circular no. K11022/460/20 16-UIDAI (Auth-II) dated 28.2.2017 — Clause 1(iii)			
127.	Authentication application audit	AUA/KUA should ensure that the authentication application of its Sub-AUAs and Sub-KUAs are audited by the Standardisation Testing and Quality Certification (STQC) Directorate of the Ministry of Electronics and Information Technology or a CERT-In-empanelled auditor and a compliance report is submitted to UIDAI. AUA/KUA should also ensure that all its Sub-AUAs and Sub-KUAs access Aadhaar Authentication facilities only through duly audited authentication	UIDAI Circular no. K11022/460/20 16-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(iv)			

| | | applications. | | | | |
| | | | | | | |

***